PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00	A1	(11) International Publication Number: WO 00/48064 (43) International Publication Date: 17 August 2000 (17.08.00)

(21) International Application Number: PCT/US00/03477

(22) International Filing Date: 10 February 2000 (10.02.00)

(30) Priority Data:

60/119,531	10 February 1999 (10.02.99)	US
Not furnished	9 February 2000 (09.02.00)	US

(71) Applicant: VASCO DATA SECURITY, INC. [US/US]; Suite 210, 1901 South Meyers Road, Oakbrook Terrace, IL 60181 (US).

(72) Inventors: HAGGARD, John, C.; Suite 201, 1901 South Meyers Road, Oakbrook Terrace, IL 60181 (US). HOORNAERT, Frank; Korbeekstraat 36, B-3061 Leefdaal (BE).

(74) Agents: MEYER, Sheldon, R. et al.; Fliesler Dubb Meyer and Lovejoy LLP, Suite 400, Four Embarcadero Center, San Francisco, CA 94111-4156 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

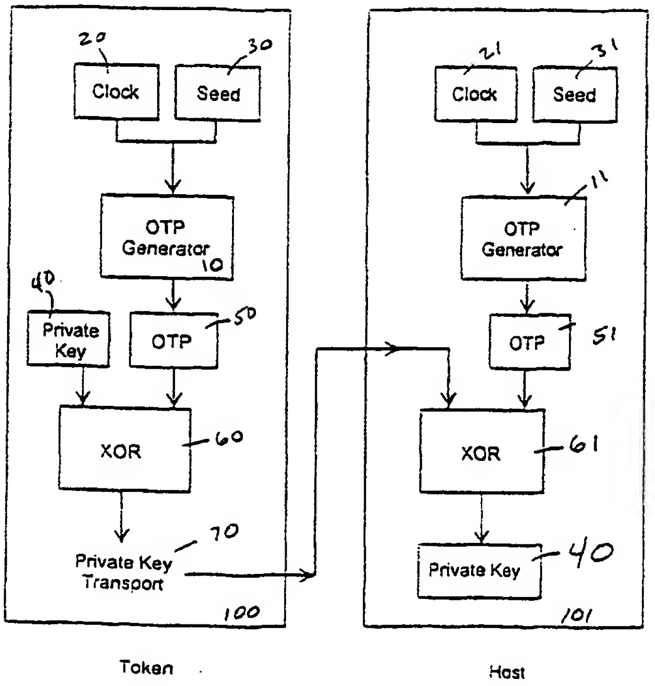
Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURITY ACCESS AND AUTHENTICATION TOKEN WITH PRIVATE KEY TRANSPORT FUNCTIONALITY

(57) Abstract

A security access and authentication token includes private key (40) transport functionality for transporting securely a private key (40) which can be used in a host to encrypt or decrypt another key or other information.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

SECURITY ACCESS AND AUTHENTICATION TOKEN WITH PRIVATE KEY TRANSPORT FUNCTIONALITY

This application claims priority to prior filed co-pending United States provisional application, No. 60/119,531, filed February 10, 1999, attorney docket no. GORD1-06359US1 SRM, entitled "SECURITY ACCESS AND AUTHENTICATION TOKEN WITH PRIVATE KEY TRANSPORT FUNCTIONALITY."

COPYRIGHT NOTICE

BACKGROUND OF THE INVENTION

Field of Invention

This invention relates to security systems. The invention is more particularly related to the secure transfer of data, passwords, keys, and other private date, for secure transfer, user validation, authorization, etc. The invention is directed towards security systems that can be used in combination with computers.

Discussion of Background

The background of the invention deals with security tokens and the like which are used for secure operations with respect to for example, a host computer. A number of patents presently describe the state of the art concerning such security systems. By way of example only, attention is drawn to the three Cargile patents and the prior art cited therein, all of which is incorporated herein by reference. The three Cargile patents include SOLID STATE KEY FOR CONTROLLING ACCESS TO COMPUTER SOFTWARE, U.S. Patent No. 4,599,489, SOLID STATE KEY FOR CONTROLLING ACCESS TO COMPUTER SOFTWARE, U.S. Patent No. 4,609,777, and SOLID STATE KEY FOR CONTROLLING ACCESS TO COMPUTER SYSTEMS AND TO COMPUTER SOFTWARE AND/OR FOR SECURE COMMUNICATIONS, U.S. Patent No. 4,819,267.

SUMMARY OF THE INVENTION

Roughly described, the private key transport (PKT) feature allows an embodiment of the token of the invention to store an application's private encryption key and to securely "transport" the key when needed. The private encryption key is sent to an application without the encryption key being exposed to the user of the token nor is it exposed in transit to the application. Once received by a host, the private encryption key can be used to lock or unlock, encrypt or decrypt other keys and other data.

Environments exists where this feature greatly reduce risks associated with deploying private key based applications. The weakness in existing systems is the reliance on a user to enter his passwords to unlock or decrypt his asymmetric private keys (i.e. RSA private keys) that are resident on his hard disks or floppy disks. The passwords are effectively the encryption keys that encrypt the private key when it is created and stored on the hard drive. The passwords also then decrypt, or unlock, the private key when loaded into memory for use in private key functions such as client authentication or signing of documents/transactions.

The weakness of static password is actually worse than one might first imagine. Traditional systems that rely on weak static passwords also have the ability to manage their problem by implementing password controls. Web based private key implementations do not have the ability to manage the weakness. There is no way to force web users to change passwords, pick good ones, or help them if they have forgotten them. The browsers rely on users to select and manage the encryption keys (i.e. passwords) that encrypted the private keys. Therefore, from a security perspective despite all the advantages that private key offers, current implementations actually are a step backward.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

Fig. 1 is a block diagram showing information flow and processes of the present invention;

Fig. 2 is a diagram of a token and host processes, interactions, and information flow according to one embodiment of the present invention; and

Fig. 3 is a flow chart describing processes performed of an embodiment of a token having combined C/R, R/O methods.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The token of the invention is preferably a Data Encryption Standard (DES) based token device. The most powerful feature of the token is that it can support up to seven different input modes (see Table 1) that support both One Time Password (OTP) paradigms - Challenge/Response and Response/Only. In addition, the token can securely transmit private keys to applications.

One Time Password Generation

In order to generate a OTP all tokens must have a secret seed value stored within the token. They must also have additional information that is variable. This additional information is what is inputted to the token when the token is used to generate a OTP. The variable input can be internally and/or externally generated. The table below identifies the seven different OTP modes of operation for the token. The table also identifies the source of the variable input given to the token for generation of the response or OTP. The challenge variable could be a value that the token receives that is used to calculate the one-time password. The time variable could be, for example, the time the token was used. The event variable could be, for example, the number of time that the token was used. Further details about OTP generation can be obtained in the above incorporated by reference Cargile patents.

Table 1

Input Modes to Token	OTP Paradigm	Source of Token Input Variable
Challenge	Challenge/Response (C/R)	External
Challenge + Event	Challenge/Response (C/R)	External & Internal
Challenge + Time	Challenge/Response (C/R)	External & Internal
Challenge + Event + Time	Challenge/Response (C/R)	External & Internal
Event	Response Only (R/O)	Internal
Event + Time	Response Only (R/O)	Internal
Time	Response Only (R/O)	Internal

All of the above modes (Table 1) use DES as a cryptographic engine for calculating the response. Each of the modes are capable of being programmed to be compatible with various standards such as ANSI X9.9, Triple-DES, or other popular tokens.

All R/O modes simply require the user to turn the unit on and, if required, to enter their personal PIN to unlock the unit. When a PIN is required the token will prompt the user for a PIN. All C/R modes utilize an advanced optical protocol enabling the user to simply hold the device in front of their monitor to read the graphical challenge presented to them. The token has a high quality keypad for manual entry of the challenge, if the monitor is not capable of a graphical interface or the user is authenticating over a phone.

Private/Personal Key Transport

One of the more important capabilities of the token is the Private Key Transport (PKT) feature (referred by cryptographic experts as "associative reading"). The PKT feature enables installations, or users, to assign a private key to a token for use by encryption applications. Use of the token by an encryption application never discloses the private key to anyone, including the user, except for the encryption application itself.

This is especially useful for applications that do not wish to be burdened with storing user's private keys. In addition, some installations do not even want users to know what their private keys are for encryption applications. Users mismanage their private secrets all the time and the result is the keys have to be changed periodically. If a user or installation assigns a private key to a user's token, the token can communicate the private key to an encryption application without having to disclose the private key during the communication (i.e. display or through a network). Hence the need to change keys are dramatically reduced.

It is important to note that this capability applies to both DES and RSA (symmetric and asymmetric) encryption algorithms.

In order to understand the significance of this feature a brief overview on how this works is needed.

Figs. 1 and 2 depict a token working with a host system running an application that has a need to use a user's private key for encryption services. The token is capable of generating a OTP as described above. Fig. 1 depicts the OTP feature in continuation with the

PKT feature, while Fig. 2 depicts the OTP feature in a single block in order to highlight the PKT feature.

The mode used (i.e. one of the seven modes of operation) to generate the OTP or Token Response is immaterial - all of the modes can be used.

When an application requests that a user supply their private key for accessing encryption services, the user operates the token in the same manner as used when authenticating (as described in the three Cargile patents incorporated herein by reference). Depending upon the OTP mode of operation the user may need to input a challenge into the token. The token will generate a token response such as for example an OTP according to the mode of operation, but will perform an additional operation before displaying a response on the token screen. The operation is illustrated above as an "XOR". The OTP 50 and the user's private key 40 are combined together (XORed) and the result is the Private Key Transport or PKT value 70. It is the PKT 70 that is displayed on the token display for the user to communicate to the host system running the encryption application. Because the internal OTP 50 is always different, the resulting PKT 70 will also always be different.

It should be noted that it is impossible to deduce the user's private key 40 with only the PKT value 70, hence the user's private key 40 is not in danger of being disclosed if the PKT 70 is disclosed.

The Host system 101 is capable of also generating the OTP 51. This is what enables the Host system 101 to validate that a particular user is who they say they are when needing to authenticate users. In the PKT case however, the host is attempting to provide the encryption application with the user's private key 40 and therefore uses the same "XOR" operation 61 to extract the private key 40 from the PKT 70. Once the "XOR" operation is completed, the encryption application can then use the private key for encryption services. Note that even though the PKT is always different, the private key extracted from each PKT generated is always the same, a requirement for symmetric encryption algorithms.

Once the encryption services have been completed the application simply erases the private key from memory, thereby protecting the private key from further disclosure.

An important point to note is that when using the token for generating PKTs, the secret OTP seed value does not have to be kept secret. The value can be openly distributed to any host system. This is not the case when using the token to authenticate user's via the token's OTP. Host systems can generate as many possible OTP's as they want, but until a physical token uses an OTP to generate a PKT, a private key cannot be generated. It should also be noted that the token can be optically programmed in the field. This feature enables the token private keys to be altered if desired.

Fig. 1 illustrates a clock 20 and seed value 30 input to the OTP generator 10. The clock 20 may be a timepiece synchronized (within any predetermined interval) with a clock 21 at a host device. Alternatively, the clock may take the form of any type of counting mechanism to provide a changing number for each or any set of OTP generations performed.

The problem that PKT feature solves is this - How can I communicate my static private key to an encryption application without using a static value that is susceptible to being trapped? The above discussion explains how the inventive token provides the solution for this problem.

XOR Operation

Token Private Key	Token Response	Private Key Transport	Host Response	Host Private Key
1	1	0	1	1
1	0	1	0	1
0	1	1	1	0
0	0	0	0	0

Exclusive OR operation (XOR) does the following. When two values are compared, if they are the same the result is a 0. If they are different the result is 1. Since we are dealing at the lowest level possible for computers the only two values possible are 0 and 1. The following table describes all possible combinations of and exclusive or operation:

1 + 0 = 1
1 + 1 = 0
0 + 0 = 0

Therefore in the above example, I have selected a token private key of '1100' and a token response value of '1010'. If I apply an exclusive or operation on these two values I get the following result - '0110', which is my Private Key Transport value. This is what happens:

1 + 1 = 0
1 + 0 = 1
0 + 1 = 1
0 + 0 = 0

This value by itself tells me nothing about the Token Private Key. '0110' in no way tells me that the real key is '1100'.

But due to the properties of the exclusive or operation, if I did this operation using the PKT and one of the original two inputs (Token Private Key and a Token Response such as an OTP) then what will be revealed is the value of the input field not used. In our case the only value that the host knows about is the Token Response (OTP) value. Therefore, the host takes the PKT value '0110' and exclusively OR's it with the host generated token response value of '1010'. This is what happens:

0 + 1 = 1

1 + 0 = 1

1 + 1 = 0

0 + 0 = 0

The result of the operation is '1100' which is equal to the Token Private Key.

Fig. 3 illustrates a process flow of a token embodiment that responds to any of C/R and R/O paradigms. At step 300, the token unit is powered up. A user inputs a password or other logon information to unlock the token (step 310). Steps 320 and 330 illustrate decision making when the token is interrogated by a system and the token determines if C/R 325 or R/O 335 processing is required. The corresponding processes are performed and the token enters a wait state 340 for further action. Upon completion of token use, the user powers down the unit (step 350).

The token includes a computing mechanism that may be initiated by a user. The following is an example of a process implemented by an initiation application resident on a token according to one embodiment of the present invention and performed by the computing mechanism. Each individual step has an associated part of the application that implements the individual step.

Parameter	Value	Note
Digipass Token	DP700	PIN code is 12541
Digipass Application	Challenge/Response	First application under the '1' - button
Activation Code	YMK3 1SUK ID5A	

Phase 1: First-Time Activation:

(a) A token application prompts the user to type the Activation Code of the selected Test Token: enter the 12-character code (see table above).

(b) The application prompts a first Challenge: enter it in the CP/700 and copy the Token response as First Dynamic Key in the application.

(c) The application prompts a second Challenge: enter it in the DP700 and copy the Token response as Second Dynamic Key in the application.

(d) The two different Dynamic Keys are verified.

(e) Both Dynamic Keys should produce the same internal secrets (referenced as SecretK2, or private key.

(f) If no error occurred, the application will flag successful PKA Activation and create context file *userfile.txt*. In this file the Activation Code is stored together with the Hash Code that is derived from the SecretK2.

Phase 2: Normal Use:

(a) The application prompts a Challenge: enter it in the DP700 and copy the Token response as Dynamic Key in the application.

(b) The Dynamic Keys is verified: if it produces an internal secret (referenced as SecretK2) that yields a Hash Code different from the stored Hash Code in context file *userfile.txt*, an error is generated.

(c) If no error occurred, the application will flag successful PKA Activation.

Resetting to Phase 1: First-Time Activation:

(a) The program may be reset to its initial state of operation by removing the context file called *userfile.txt*.

(b) The application provides a button 'Clear Context File' to this end. Pressing it once will delete the file.

(c) The next time the 'Start' button is pressed, the First-time Activation phase will proceed.

Accordingly, the present invention provides for an inventive private key transport feature, and having industrial applicability in a wide range of business, security, and other technical fields for secure transmission of data, encryption codes, passwords, keys, etc. Other features, aspects and objects of the invention can be obtained from a review of the figures.

The present invention may be conveniently implemented using a conventional general purpose or a specialized digital computer or microprocessor programmed according to the teachings of the present disclosure, as will be apparent to those skilled in the computer art.

Appropriate software coding can readily be prepared by skilled programmers based on the teachings of the present disclosure, as will be apparent to those skilled in the software art. The invention may also be implemented by the preparation of application specific integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be readily apparent to those skilled in the art.

The present invention includes a computer program product which is a storage medium (media) having instructions stored thereon/in which can be used to control, or cause, a computer to perform any of the processes of the present invention. The storage medium can include, but is not limited to, any type of disk including floppy disks, optical discs, DVD, CD-ROMs, microdrive, and magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, DRAMs, VRAMs, flash memory devices, magnetic or optical cards, nanosystems (including molecular memory ICs), RAID devices, remote data storage/archive/warehousing, or any type of media or device suitable for storing instructions and/or data.

Stored on any one of the computer readable medium (media), the present invention includes software for controlling both the hardware of the general purpose/specialized computer or microprocessor, and for enabling the computer or microprocessor to interact with a human user or other mechanism utilizing the results of the present invention. Such software may include, but is not limited to, device drivers, operating systems, and user applications. Ultimately, such computer readable media further includes software for performing the present invention, as described above.

Included in the programming (software) of the general/specialized computer or microprocessor are software modules for implementing the teachings of the present invention, including, but not limited to, performing XOR operations, OTP generation, and the display, storage, or communication of results according to the processes of the present invention.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

WHAT IS CLAIMED AND DESIRED TO BE SECURED BY LETTERS PATENT OF THE UNITED STATES IS:

1. A token for generating a private key transport value, comprising:

a one-time password (OTP) generator configured to produce a password each time the OTP generator is invoked;

a private key (PK) storage device configured to maintain storage of a private key;

a combinatorial device configured to combine said private key stored in said PK storage device with a password produced by said OTP generator to produce a private key transport (PKT) value; and

a transport mechanism configured to at least one of display and communicate said PKT value.

2. The token according to Claim 1, wherein said OTP generator comprises:

a clock device configured to produce a clock value;

a seed storage mechanism configured to store a seed value; and

a second combinatorial device configured to combine said seed value and a clock value produced by said clock device to produce an OTP.

3. The token according to Claim 2, wherein said clock device varies said clock value at a predetermined time interval.

4. The token according to Claim 1, wherein said OTP generator produces a different password each time the OTP generator is invoked.

5. The token according to Claim 1, wherein said PK storage device comprises a non-volatile memory that stores said private key.

6. The token according to Claim 1, wherein said combinatorial device is an x-or mechanism.

7. The token according to Claim 1, wherein said transport mechanism is an optical device that transmits an optical protocol signal allowing communication of said PKT from said token to a remote device capable of receiving said optical protocol signal.

8. The token according to Claim 1, wherein said transport mechanism is a display device configured to display said PKT, thereby allowing any one of (1) a user to read and utilize said PKT, and (2) a receiving device to scan said PKT.

9. The token according to Claim 1, wherein said OTP generator is synchronized with a OTP at a host device that receives said PKT.

10. The token according to Claim 1, further comprising:

a private key input mechanism configured to receive a private key from any one of a user and an installer of said token; and a saving mechanism configured to save the received private key in said private key storage device.

11. The token according to Claim 1, further comprising an input mechanism that receives an input condition that invokes said generating a private key transport value.

12. The token according to Claim 11, wherein said input condition comprises any one of a challenge, event, time, and any combinations of challenge, event and time, including (1) event and time, (2) challenge and event, (3) challenge and time, and (4) challenge and event and time.

13. The token according to Claim 1, wherein said generating a private key transport value is performed based on any one of an event, a time, and a combination of event and time.

14. The token according to Claim 1, wherein said OTP generator is synchronized with at least one second OTP generator at a host device that receives said PKT value.

15. A host device, comprising:

a one-time password (OTP) generator configured to produce a password each time the OTP generator is invoked;

a private key transport (PKT) reception mechanism configured to receive a PKT value having an encrypted private key; and a combinatorial device configured to combine said PKT value with a password generated by said OTP generator to derive the private key.

16. The host according to Claim 15, wherein said combinatorial device is an x-or mechanism configured to x-or said PKT value with said OTP.

17. The host according to Claim 15, wherein said combinatorial device is a series of x-or gates, a first input of each gate inputting one binary digit of said PKT value, and a second input of each gate inputting one binary digit of said OTP.

18. The host according to Claim 15, wherein said PKT reception mechanism is an optical receiver configured to receive an optical protocol signal containing said PKT value.

19. The host according to Claim 15, wherein said OTP generator produces a different password each time the OTP generator is invoked.

20. The host according to Claim 15, wherein said OTP generator is synchronized with a OTP generator associated with a token device that produces the received PKT value.

21. A method of maintaining and transmitting a private key, comprising:

producing a one-time password (OTP);

retrieving a private key from a storage device;

combining said OTP and said private key to produce a private key transport (PKT) value; and

transmitting said PKT value to a reception mechanism.

22. The method according to Claim 21, wherein said step of combining comprises x-oring said OTP and said private key to produce said private key transport (PKT) value.

23. The method according to Claim 21, wherein said step of producing a one time password, comprises:

retrieving a seed value from a storage device;

producing a clock value; and

combining said clock value and said seed value to produce said OTP.

24. The method according to Claim 21, further comprising the step of:

synchronizing a OTP generator configured to produce said OTP with a OTP generator used to de-crypt said PKT value.

25. A method of receiving a private key, comprising the steps of:

receiving an encrypted private key;

producing a one-time password (OTP); and

combining said OTP and the received encrypted private key to produce the private key.

26. The method according to Claim 25, wherein said step of combining comprises x-oring said OTP and said private key to produce said private key.

27. The method according to Claim 25, wherein said step of producing a one-time password, comprises:

retrieving a seed value from a storage device;

producing a clock value; and

combining said clock value and said seed value to produce said OTP.

28. The method according to Claim 25, further comprising the step of:

synchronizing a OTP generator configured to produce said OTP with a OTP generator used to produce said encrypted private key.

29. A system for providing secure access and authorization, comprising:

a token, comprising,

a private key transport (PKT) generation device configured to generate a PKT value that securely encrypts a private key, and

a transport mechanism configured to at least one of (1) display said PKT value, and (2) communicate said PKT value; and

a host device, comprising,

a PKT reception device configured to accept said PKT value whether (1) input by a user of said token, or (2) communicated to said reception device from said transport mechanism, and

a decryption mechanism configured to decrypt said PKT value to derive said private key; and

an authorization mechanism configured to authorize any one of execution of a software program, user validation (authentication), and access to a file, account, or other device based on the derived private key.

30. The system according to Claim 29, wherein:

said PKT generation device comprises a first one-time password (OTP) generator and a forward algorithm that combines a first OTP generated by said first OTP generator with said private key to produce said PKT value; and

said decryption mechanism comprises a second OTP generator and a reverse algorithm that combines a second OTP generated by said second OTP generator with said PKT value to derive said private key.

31. The system according to Claim 30, wherein said forward algorithm is an x-or operation between said first OTP and said private key.

32. The system according to Claim 30, wherein said reverse algorithm comprises an x-or operation between said second OTP and said PKT value.

33. The system according to Claim 30, wherein :

said PKT generation device includes,

a seed value stored in non-volatile memory,

a clock, and

a combinatorial mechanism configured to combine said seed value and a clock value from said clock to produce said first OTP; and

said decryption mechanism includes,

a second seed value stored in a second non-volatile memory,

a second clock, and

a second combinatorial mechanism configured to combine said second seed value and a second clock value from said second clock to produce said second OTP.

34. The system according to Claim 33, wherein the PKT generation device clock and the decryption mechanism clock are synchronized.

35. The system according to Claim 29, wherein said authorization mechanism allows transfer of data maintained in said private key to any one of (1) storage space on said host or a connected device, and (2) another application at said host or connected device.

36. In a system having multiple users or groups of users (users) and any number of user accounts, invocable software programs, and/or other devices needing secure access/authentication, each of said accounts, software programs, and/or other devices being accessible at least one level by any one or more of said users, said system comprising:

at least one token for each of said multiple users, each token configured to generate and transmit a private key transport (PKT) value containing an encrypted private key;

at least one host device configured to,

accept a PKT value transmitted from a user's token,

decrypt the accepted PKT value to derive a private key associated with the user's token, and

grant access to a file, program, account, or other device requested by a user of the token, said access granted according to authorization associated with the derived private key.

37. The system according to Claim 36, wherein each token device comprises:

a one-time password (OTP) generator configured to produce a password each time the OTP generator is invoked;

a private key (PK) storage device configured to maintain storage of a private key;

a combinatorial device configured to combine said private key stored in said PK storage device with a password produced by said OTP generator to produce said private key transport (PKT) value; and

a transport mechanism configured to at least one of display and communicate said PKT value;

wherein the private key stored in said PK storage device of any one token is associated with the user of said one token.

38. The system according to Claim 16, wherein each host device comprises:

a one-time password (OTP) generator configured to produce a password each time the OTP generator is invoked;

a private key transport (PKT) reception mechanism configured to receive PKT value having an encrypted private key; and

a combinatory device configured to combine said PKT value with a password generated by said OTP generator to derive the private key;

wherein said derived private key provides access and/or authorization to any of accounts, programs, or other devices said user is authorized to access.

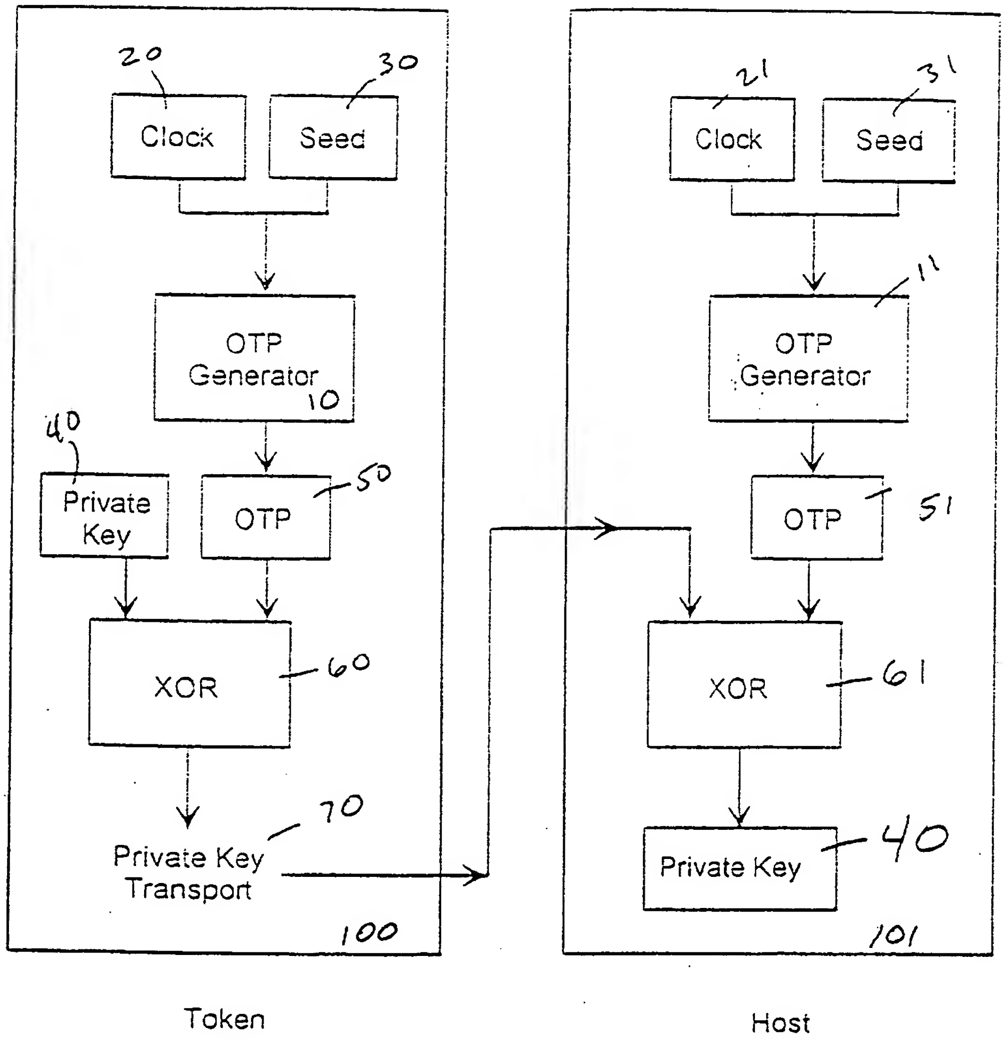

20
30
Clock
Seed
OTP Generator
10
40
Private Key
OTP
50
XOR
60
70
Private Key Transport
100
Token
21
31
Clock
Seed
11
OTP Generator
OTP
51
XOR
61
Private Key
40
101
Host

Fig. 1

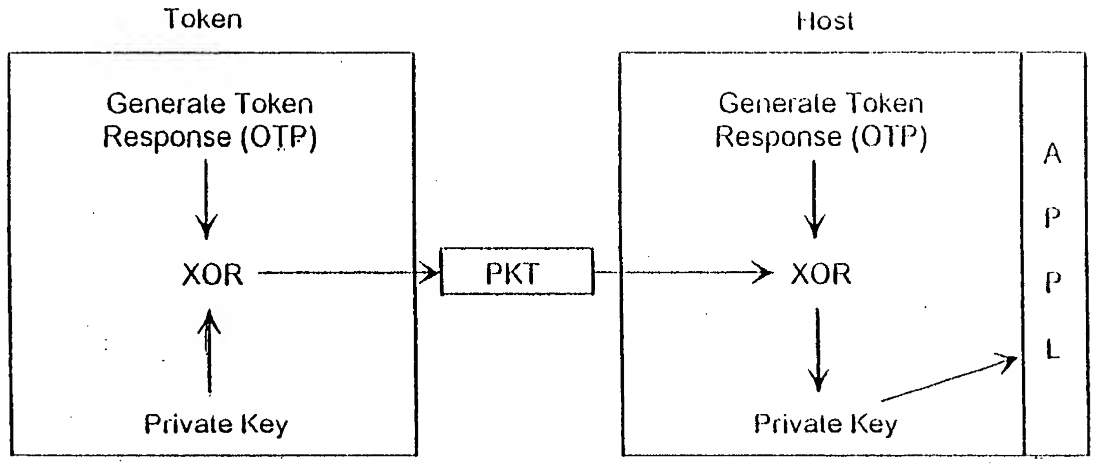

Token
Generate Token Response (OTP)
XOR
Private Key
PKT
Host
Generate Token Response (OTP)
XOR
Private Key
A
P
P
L

Fig. 2

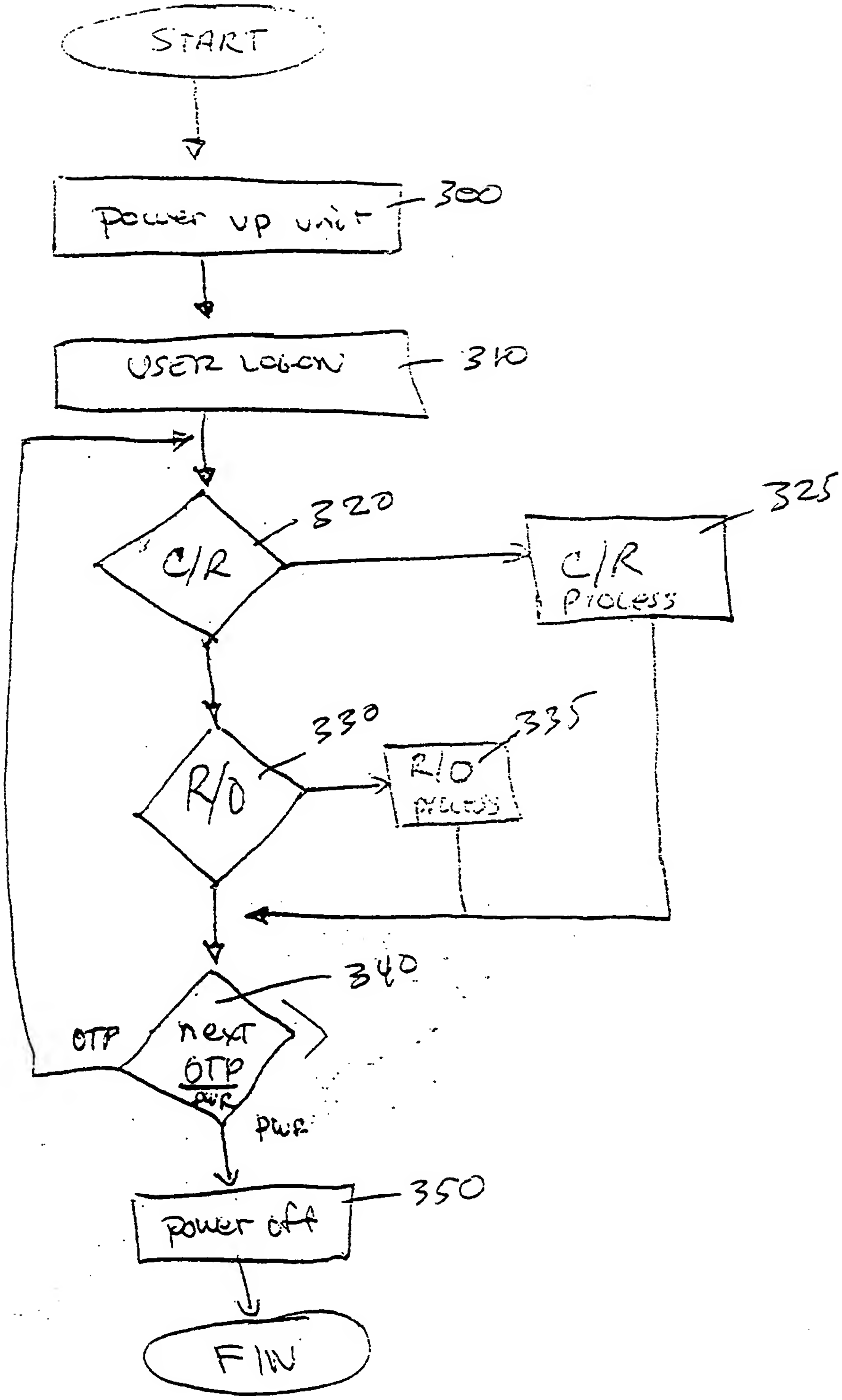

START
power up unit
300
USER LOGON
310
C/R
320
C/R process
325
R/O
330
R/O process
335
next OTP
PWR
340
OTP
PWR
power off
350
FIN

FIG. 3.

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 00/03477

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 657 388 A (WEISS KENNETH P) 12 August 1997 (1997-08-12)	29,35,36
A	abstract column 4, line 27 -column 6, line 28 figures 1,2 ---- -/--	1-5,7, 9-15, 18-21, 23-28, 30,33, 34,37,38

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 21 June 2000	Date of mailing of the international search report 28/06/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Jacobs, P

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/03477

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 819 267 A (CARGILE WILLIAM P ET AL) 4 April 1989 (1989-04-04) cited in the application	29,35,36
A	abstract column 2, line 18 - line 54 column 5, line 34 -column 7, line 68 column 12, line 15 -column 19, line 35 figures 1,7-10	1-6, 8-17, 19-28, 30-34, 37,38
X	EP 0 566 811 A (IBM) 27 October 1993 (1993-10-27)	29,35,36
A	abstract column 8, line 7 -column 11, line 55	1-5,8, 10-13, 21,23, 25,27,37
A	US 4 799 258 A (DAVIES DONALD W) 17 January 1989 (1989-01-17)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intl. ional Application No
PCT/US 00/03477

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5657388 A	12-08-1997	US 5485519 A	16-01-1996
		AU 681500 B	28-08-1997
		AU 1992495 A	03-10-1995
		CA 2183629 A	21-09-1995
		EP 0750814 A	02-01-1997
		JP 9510561 T	21-10-1997
		WO 9525391 A	21-09-1995
		US 5479512 A	26-12-1995
US 4819267 A	04-04-1989	US 4599489 A	08-07-1986
		AT 42844 T	15-05-1989
		AU 4062685 A	10-09-1985
		DE 3569994 D	08-06-1989
		EP 0172239 A	26-02-1986
		JP 61501291 T	26-06-1986
		WO 8503785 A	29-08-1985
		US 4609777 A	02-09-1986
		EP 0253885 A	27-01-1988
		WO 8703977 A	02-07-1987
EP 0566811 A	27-10-1993	US 5347580 A	13-09-1994
US 4799258 A	17-01-1989	GB 2154344 A,B	04-09-1985